https://www.financial-planning.com/news/this-is-the-biggest-cybersecurity-threat-for-wealth-firms

This is the biggest cybersecurity vulnerability firms face
By Rob Burgess
April 01, 2025, 5:10 p.m. EDT

A wealth management firm can have all the most sophisticated cybersecurity applications available on the market, but experts say the most significant weakness is still simple user error.

Studies have shown the vast majority of cyberattacks start with email.

Jacob W. Anderson, president of Beyond Ordinary Software Solutions, told Financial Planning targeted human exploitation has become an "everyday threat."

"We see more email and other forms of communication that explicitly target the trust humans have for each other," he said. "This has made cybersecurity more of a social psychology exercise than a perimeter security problem."

In a recent joint webinar with Schwab Advisor Service and Halbert Hargrove, Patrick Hennessey, director of business consulting and education at Schwab Advisor Services, said while fraud and scams are interrelated, they are not the same. He said both tend to stem from some sort of information security or cybersecurity breach or intrusion, or "our own sometimes sloppy or negligent behavior."

"Fraud can come down to someone impersonating you to try and get at your information or assets," he said. "With scams, though, you're often an unwitting participant, so someone is playing you. They're using psychology and social engineering tactics to try and get something from you, typically information that they then can leverage to get at your money, your assets."

Hennessey said with both frauds and scams, the perpetrators are "trying to get little morsels of information that they can use to do greater damage." He said intrusions into email accounts are the "No. 1 attack vector that we see."

"We might overshare information or be too cavalier with how we protect our information," he said.

AI creates 'novel vectors of risk'
Roberta Duffield, director of intelligence at risk intelligence platform Blackbird.AI, told Financial Planning that "AI has created novel vectors of risk that significantly increase their effectiveness."

"Fundamentally, scams are a numbers game," she said. "Even if only one person in 10,000 falls for a deception, this counts as a win for the scammer. If criminals

can leverage AI to decrease the amount of time it takes to reach higher volumes of people, their likelihood of success exponentially increases."

For instance, Duffield said an AI agent can use large language model (LLM) technology to hold extensive, authentic conversations online in real time that adapt to the responses a human gives them, or send out thousands of individually crafted and personalized phishing messages, all without needing extensive oversight.

"This allows scammers to engage with many potential victims simultaneously, dramatically increasing the scale — and success — of their operations," she said. "A successful scam is the one that goes undetected. Exploiting our cognitive biases to appear trustworthy, recognizable or personally appealing, means victims are less likely to question the scam's provenance. Our cognitive biases are predisposed to assume the scammer is legitimate if they already know their name, personal information or other details about their life, such as a personally addressed email claiming to be from their local bank branch."

Scams that target a person's known interests and activities can also capture their attention more easily, said Duffield. To this end, AI can be leveraged to sift through data scraped from social media, data breaches and public records to customize email or text message content, allowing scammers to tailor fraudulent content to specific audiences, she said.

"For instance, a social media user known to be interested in digital currency trading may be more amenable to solicitation from a fraudulent crypto investor offering their services," she said. "The speed and accuracy to which AI can complete these tasks far outstrip a human's ability to do so. Personalization can be as general as 'residents of North Carolina,' or highly targeted — such as a phone call from a 'lawyer' addressing you by name, stating that your granddaughter is in jail and urgently needs bail money."

How to protect against these intrusions

Anderson said personnel at his firm must be trained in understanding how and why these threats occur. Counting training and software, he said his firm spends anywhere from $300,000 to $400,000 annually on cybersecurity.

"We have to utilize filtering tools at the perimeter to attempt the capture and sequestration of these types of attacks before they can materialize," he said. "Then when an attack does materialize, we have to utilize very sophisticated behavior tools that recognize and prevent humans from being exploited by these actors."

During the webinar, Nick Mancini, senior consultant of business consulting and education at Schwab Advisor Services, said to protect against email intrusions, passwords should be long, somewhere between 12 and 15 characters.

"Fraudsters today have technology that they can often use to guess or crack a

password, and if that password is six or eight characters, it might be able to be guessed in a matter of minutes using this technology," he said. " Yet simply pushing it to 12 or 15 characters, using that same technology, could take years, or, in some cases, even decades."

Mancini said ideally passwords should be unique for each platform. He said this is important because when there is a breach where passwords and user IDs are exposed, these bad actors sell that information back and forth to one another over the internet.

"They'll plug it into technology that, in an instant, can go out and test that user ID and password on dozens or hundreds of different websites," he said. "Very often they're able to get in because we've reused our password."

Password managers can also be purchased in the various app stores and securely store passwords using deep encryption, said Mancini.

"They'll let us know if we're reusing a password," he said. "They'll let us know if a platform has had a compromise. … They're also fantastic at generating passwords. … I let go of knowing my passwords years ago."

Also during the webinar, Shane Cummings, wealth advisor and director of technology and cybersecurity at Halbert Hargrove, said in addition to a password manager, multifactor authentication (MFA) with time-based codes are an essential step to help ensure security.

"When you set that form of MFA up, it's powerful, and also lessens your chance of that MFA being compromised," he said.